FARSIGHT SECURITY

July 16th, 2017

To: Mr. Ajit Pai, FCC Chairman
Ms. Mignon Clyburn, Commissioner
Mr. Michael O'Rielly, Commissioner
CC: Ms. Marlene H. Dortch, Secretary
[filed electronically via https://www.fcc.gov/ecfs/]

Subject*:* Comments on "Restoring Internet Freedom" NPRM (WC Docket No. 17-108, comments due July 17th, 2017) as announced at https://apps.fcc.gov/edocs_public/attachmatch/DOC-344614A1.pdf

Dear Chairman Pai, Commissioners Clyburn and O'Rielly, and Secretary Dortch:

It is our pleasure to offer Farsight Security's comments on the above captioned Notice of Proposed Rule Making (NPRM).

Part I. Context for These Comments

Section 1) Our Company:

Farsight Security, Inc., is an Internet security company headquartered in San Mateo, California. Leveraging our deep Domain Name System (DNS) expertise, Farsight Security offers real-time Passive DNS solutions that provide critical context to significantly increase the value of prepackaged reputation & threat feeds, and other threat intelligence. At Farsight, we are committed to finding new ways to secure the world's digital infrastructure while fully respecting and protecting the privacy of all law-abiding Internet users. More information about Farsight Security, Inc., can be found online at our website.[1]

Section 2) Background of Those Submitting These Comments:

Dr. Paul Vixie is the Chief Executive Officer and Chairman of the Board of Farsight Security, Inc. He's previously served as President, Chairman, and Founder of Internet Systems Consortium (ISC), as President of MAPS, PAIX and other businesses, as CTO of Abovenet/MFN, and serve on the boards of several for-profit and non-profit companies. He has previously served on the ARIN Board of Trustees, including serving as Chairman in 2008 and 2009, and he was a founding member of ICANN Root Server System Advisory Committee (RSSAC) and ICANN Security and Stability Advisory Committee (SSAC). He operated the ISC's F-Root name server for many years, and he is a member of Cogent's C-Root team. He's also a sysadmin for a leading industry cybersecurity information sharing forum, OpSec Trust. He earned his Ph.D. from Keio University for work related to DNS and DNSSEC, and was named to the Internet Hall of Fame in 2014. His comments today are in his capacity as Farsight CEO and Chairman of the Board, and reflect both his own personal perspective on these matters and Farsight Security, Inc.'s official company perspective.

Ms. Merike Käo: Merike Käo is the CTO of Farsight Security, responsible for developing the company's technical strategy and executing its vision. Prior to joining Farsight Security, Merike held positions as CISO for Internet Identity (IID), and founder of Doubleshot Security, which provided strategic and operational guidance to secure Fortune 100 companies. She led the first security initiative for Cisco Systems in the mid 1990s and authored the first Cisco book on security, translated into more than eight languages and leveraged for prominent security accreditation programs such as CISSP. In 2007, Merike was instrumental in fostering cooperation and trust among the global ISP liaisons during the cyber attacks against Estonia. Merike is a member of the IEEE, a pioneer member of ISOC, and has been an active contributor in the IETF since 1992. She is deeply rooted in the Internet technical community, having supported organizations such as NANOG, APNIC, RIPE, ICANN, IGF, ISOC, and Interop. She was named an IPv6 Forum Fellow in 2007 for her continued efforts to raise awareness of IPv6 related security paradigms. She is on ICANN's Security and Stability Advisory Council (SSAC) and the FCC's Communications Security, Reliability and Interoperability Council (CSRIC). Merike earned a MSEE from George Washington University and a BSEE from Rutgers University. Merike was appointed to the ARIN Board of Trustees in 2016 to serve a one-year term from 1 January 2017 to 31 December 2017. Her comments today are offered in her role as Farsight's CTO, and are not meant to represent the perspective of any other organization.

[1] https://www.farsightsecurity.com/

Part II. Overall Support for the "Restoring Internet Freedom" NPRM.

Section 3) Overall Summary Position:

While we understand and appreciate the concerns that have been expressed around "net neutrality," Farsight Security supports the Commission's efforts to end public utility-style regulation of the Internet, and to return to the "light regulatory approach" that dated from the Clinton administration. We believe that a light regulatory touch is essential to continued Internet growth, competitiveness, efficiency, security and stability, and need not directly result in problematic ISP traffic management practices.

We also are in favor of entrusting the FTC with responsibility for Internet privacy protection. The FTC has done excellent work in consumer privacy to-date, including in the anti-spam area, and our expectation is that fully returning Internet privacy to their remit will forestall any potential bureaucratic "turf wars" and allow for consistent and synergistic investigations into any privacy issues that may arise in the future.

That said, we do have comments on a number of technical points in your NPRM, hence our filing today.

Part III. Specific Technical Feedback

Section 4) NPRM Paragraph 37: This paragraph reads:

> *[...] Second, the Title II Order found that DNS [fn 92] and caching [fn 93] used in broadband Internet access service were just used "for the management, control, or operation of a telecommunications system or the management of a telecommunications service." [fn 94] The Commission has previously held this category applies to "adjunct-to-basic" functions that are "incidental" to a telecommunications service's underlying use and "do not alter [its] fundamental character." [fn 95] As such, these functions generally are not "useful to end users, rather than carriers." [fn 96]* ***We seek comment on how DNS*** *and caching* ***functions are now used, whether they benefit end users, Internet service providers, or both, and whether they fit within the adjunct-to-basic exception. How would broadband Internet access service work without DNS*** *or caching?* ***Would removing DNS have a merely incidental effect on broadband Internet users, or would it fundamentally change their online experience?*** *[emphasis added]*

We begin by considering the highlighted portion of paragraph 37 quoted above, intentionally omitting commentary on caching.

Because the critical role played by the Domain Name System is easily overlooked, let us be blunt for just a moment: without the Domain Name System, **the Internet (at least as we know it) could not exist.**

Let us explain what we mean by this via a brief example... Consider just the Internet's most popular site, Google. Most of us visit Google (or a similar Internet search engine) multiple times a day from our web browser.

With the Domain Name System, you're able to easily get to Google by just typing in google.com.

Without the Domain Name System you'd have to remember and enter a numeric IPv4 address such as 172.217.7.228, or, even worse, an IPv6 address such as 2607:f8b0:4004:802::2004. This would fundamentally (and negatively) change a broadband Internet user's online experience.

What about "workarounds?" (We discount the ingenuity of the Internet at our peril.) For example, in a hypothetical DNS-less world, some people might try to "get by" by "hard coding" the IP address of a search engine into their web browsers, and then letting an IP-address-only search engine "bootstrap" everything else they might be seeking -- at least on the web. That would be a highly "search-engine-dependent" alternative Internet reality, and one where no one would voluntarily elect to live, if only because the Internet is much more than just the web.[2] What about email, for example, or instant messaging? Virtually **all** Internet applications expect domain names. Virtually **none** of those applications (other than the web) can be configured to use search engines as a sort of "bailing wire and duct tape" workaround that might enable a hypothetical DNS-less Internet environment.

[2] Going to an IP-address-only web environment would necessitate foregoing the use of SNI (see https://en.wikipedia.org/wiki/Server_Name_Indication) and would thus accelerate the need for uptake of IPv6 addresses.

We will also concede that some highly-specialized environments, such as Tor's hidden services sites, do exist and function without relying on the Domain Name System. Sadly, dot onion addresses are typically as cryptic and non-human-friendly as raw IPv4 or raw IPv6 addresses (unless significant effort is put into brute force discovery of a marginally-better Tor address for a given resource). As a *practical-and-broadly deployed* technology, when it comes to Internet addressing, Zooko[3] was right.

Section 5) DNS Other-Than-For-Addressing-Related Uses:

We now consider one other part of paragraph 37 from the NPRM. The FCC asked:

> ***Are there other ways that DNS** or caching **are used for "for the management, control, or operation of a telecommunications system"?*** [emphasis added]

We would be remiss if we did not note that the DNS is widely used as more than "just" an addressing scheme (important as that basic role may be). We'll now provide a couple of examples of what we mean by this.

DNS-used-as-a-distributed-database: The Domain Name System, while originally conceived of as a way to map symbolic domain names to IP addresses, can also be used for "off-label" purposes as a "general purpose distributed database." For example, DNS can be used to store and provide reputation information via various blocklists (blocklists contain domain reputation data, and are meant to help sites block spam, phishing, malware and other unwanted traffic). That is a clear example of "DNS used for the management, control or operation of a telecommunication system," even if that's a re-purposement beyond the originally-intended scope of the Domain Name System.

"DNS Firewalls" Created Using DNS Response Policy Zones (RPZ): Another example of "DNS used for the management, control or operation of a telecommunication system" can be seen in Response Policy Zones. Response Policy Zones may be used to intentionally block or redirect attempts to access domains based on site policies codified in Response Policy Zone ("RPZ") files.[4] For example, end users may be protected from accidentally stumbling into malware or phishing sites by automatically redirecting their web browser to a non-malicious educational warning page.

Section 6) NPRM Paragraph 30: We would also like to comment on paragraph 30 from the NPRM. That paragraph reads:

> *For another, **Internet service providers routinely change the form or content of the information sent over their networks—for example, by using firewalls to block harmful content or using protocol processing to interweave IPv4 networks with IPv6 networks.** The Commission has acknowledged that broadband Internet networks must be reasonably managed since at least the 2005 Internet Policy Statement. [fn 77] We believe that consumers want and pay for these functionalities that go beyond mere transmission—and that they have come to expect them as part and parcel of broadband Internet access service. We seek comment on our analysis. **What constitutes a "change in the form" of information?** If not the protocol-processing for internetworking-considered an enhanced service under the Computer Inquiries—how should we interpret this phase so it carries with it independent meaning and is not mere surplusage? **How could we plausibly conclude that it is not a "change in the ... content" to use of firewalls and other reasonable network management tools to shield broadband Internet users from unwanted intrusions and thereby alter what information reaches the user for the user's benefit?** We seek comment on other ways in which Internet service providers change the form or content of information to facilitate a broadband Internet user's experience on line.* [emphasis added]

We would suggest that "interweaving IPv4 networks with IPv6 networks" is not a "change in the form" of information, it merely the interconnection of two alternative bearer services. Think of it as being like a ramp between a city street and an interstate highway. Traffic (or data) flows over the junction, but the content (application traffic) isn't changed just by shipment, or by the transition from one roadway (or one IP protocol version) and another. More plainly, if a 20 foot metal shipping container gets carried on a flatbed truck, or on a rail car, or on a container ship, that's of no matter. The contents of the shipping container aren't normally changed by

[3] https://en.wikipedia.org/wiki/Zooko%27s_triangle

[4] https://dnsrpz.info/

that transport, and the customer typically can't even tell how "their" container may have been carried without inspecting shipping documents. If a transportation company were to "scramble the contents" of the container on some hypothetical gigantic shipping container-sized agitator, or "barbeque" the loaded container in some gargantuan oversized industrial oven, those sort of activities would "change the form" of the container's contents. Mere use of a different technology to move a container -- or a packet of data -- from point A to point B normally will not. (Increasingly, hop-by-hop and end-to-end encryption technically ensures that the integrity of transmissions over the Internet cannot be impaired)

Likewise, blocking unwanted traffic with a firewall or spam filter actually *preserves* the usability of the content the customer wants, and is no different than a hotel room door having a lock to keep out intruders or a screened window to keep out bugs -- filtering is sometimes intrinsic to the delivery of a service, and to the preservation of its usability. Protective filtering (whether by firewall, anti-spam service, or other mechanism) PREVENTS changes to the usability of online content, rather than allowing junk traffic to pollute and overwhelm a service, destroying its essence and usability. It is critical that ISPs retain the discretion to offer such services to best meet their customer's needs, and to protect their infrastructure and services from attacks.

At the same time, ISPs should NOT have the unilateral discretion to weigh in and selectively "censor" or limit lawful Constitutionally-protected expression the consumer desires to receive. This principle is likely best accomplished by making any filtering of unwanted traffic user-supressable (except for mandatory/universal filtering of online child abuse materials, sometimes mistakenly referred to as "child pornography"[5]).

We were very heartened to see the Commission state in paragraph 79 that "We emphasize that we oppose blocking lawful material." We believe that most ISPs will understand and respect the Commission's perspective on this point without the need for formal rulemaking at this time. If that proves incorrect, the Commission obviously could undertake followup regulatory action at a later date.

We'd also note, for clarity, that in providing user filtering, ISPs should not be required to potentially spin up an infinite variety of narrowly-tailored filtering options to meet a potentially infinitive variety of customer requirements -- a customer who's dissatisfied with the filtering options available from their ISP should have the ability to opt out of the provider's filtering and then do their own filtering. Transparency and choice cure many potentially difficult ills.

Section 7) Paragraph 36:

Paragraph 36 once again finds the Commission wrestling with definitions and attempting a dialectical dissection of "transmission... of information" vs a "capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information."

We understand that this attention is based in part on the *Title II Order's* earlier interpretation of the *Telecommunications Act of 1996* and the *Title II Order's* analysis of "marketing and pricing strategies." That, apparently, is how we've come today to be specifically asking if "[...] Internet service providers' marketing has decidedly changed in recent decades."

Marketing and advertising considerations should not drive the formulation of network policies. Most consumers have long ago come to distrust and "tune out" most marketing targeted at them -- that's why an ad blocking program is the number one add-on for one popular web browser,[6] and why many consumers don't trust the advertising they do still see.[7] The FCC should take this into consideration.

At the risk of overgeneralization, what broadband consumers typically want is simple: *a fast connection that's always available and offered at a fair price.* If you can deliver those three things, consumers will flock to your broadband service. If your connections are slow, or your connections are up and down like a yo-yo, or your pricing acts to gouge the end user, they'll take their business elsewhere. Advertising may attempt to "razzle-dazzle" consumers by "reframing" those requirements or attempting to introduce

[5] https://www.interpol.int/Crime-areas/Crimes-against-children/Online-child-abuse-Q-As

[6] https://addons.mozilla.org/en-US/firefox/extensions/?sort=users

[7] https://www.forbes.com/sites/marketshare/2013/02/26/this-just-in-a-lot-of-people-dont-trust-advertising/

new "requirements," but at root, "fast/stable/affordable" is still the "magic recipe" that all successful broadband providers *must* deliver. Marketing may endeavor to support that operational and financial reality (or attempt to gloss over operational or financial deficiencies in delivering those key ingredients) but ultimately "fast/stable/affordable" will always be what counts, not advertising.

We also note that connection speed was explicitly mentioned in this paragraph. Please note that most consumer systems, and most consumer applications, are NOT tuned to the point where they can saturate a gigabit link or other high speed broadband connection even if they have one.[8] In many consumer broadband networks, the business model is based on oversubscription since in virtually all cases most of that provisioned capacity will never be routinely used.

Some of the problem is packet loss. Even miniscule levels of packet loss means that going fast is impossible. High throughput networks must have zero packet loss (as is true for research networks like Internet2 and the campus networks that connect to them). If you want to make concrete progress toward improved Internet speed, shine a spotlight on packet loss levels, and encourage application developers to collect and routinely disseminate application performance information.[9]

Application developers, just like car designers, also need to be challenged to develop high throughput products. If the market seems to only need a fleet of "econoboxes" to go from home to the office to the supermarket to home, we'll never have fleets of affordable Porsches and Ferraris. If a Commission goal is to have consumers actually effectively leveraging gigabit+ connections to the home at some point -- bringing realized broadband speeds into the 21st century -- operating systems and applications will need to be routinely tuned and enhanced to meet that expectation.[10]

Suitable incentives should reward operating systems and applications that demonstrably deliver those objectives.

Section 8) Paragraphs 82-87 (Throttling and Prioritization)

Dr. Joe St Sauver, a person who'd previously been appointed to the Commission's Communication Security, Interoperability and Reliability Council (CSRIC)[11] and who is now a Scientist with Farsight, had previously filed comments in a personal capacity with the FCC on 7/15/2014 relating to "Protecting and Promoting the Open Internet," see https://ecfsapi.fcc.gov/file/7521480410.pdf

Farsight supports and hereby reiterates the relevant portions of that filing by reference when it comes to the current inquiry's paragraphs 82-87, namely:

- Jitter-, Latency-, and Loss-Sensitive Traffic Must Be Able To Continue To Be Prioritized (And Thus Protected) From Competing Bulk Flows
- Different Types Of Connectivity Are Not All Alike & Throughput is Not Always Within the ISP's Control
- [The FCC Shouldn't] Prevent ISPs From Offering a Rich Portfolio of Market Options

We believe that filing remains relevant today, and urge you to see that earlier filing for more details around these points.

[8] This is not a unique phenomena limited to consumer broadband networking, either -- higher education discovered this issue when they deployed Internet2, offering loss-free, lightly-loaded, high-capacity links, only to find typical faculty members and graduate students saw no significant increase in research project throughput without attention from network performance experts. That work on network performance continues today, see for example https://www.internet2.edu/vision-initiatives/initiatives/performance/

[9] Naturally, performance data collection and data dissemination should be opt-in, and require informed consent.

[10] An outstanding resource for those interested in system and network performance tuning is http://fasterdata.es.net/

[11] https://apps.fcc.gov/edocs_public/attachmatch/DA-13-985A1.txt

Section 9) Conclusion:

Thank you for the opportunity to weigh in on this NPRM. In summary, we support the Commission's current NPRM and agree that the FTC is the right place for Internet privacy protection work.

More specifically, as you craft the Commission's new policies, we hope that you will:

-- Protect ISP's ability to offer recursive resolver ("DNS") service for their customers -- without it, the Internet wouldn't work

-- Protect ISP's ability to use DNS (including things like DNS Response Policy Zones and DNS blocklists) as a way to control unwanted traffic and manage their networks. ISPs must be able to filter unwanted traffic (such as spam, malware, phishing and DDoS attack traffic) so as to maintain usability of the Internet -- without it, the Internet may descend into chaotic unusability.

-- Please do not cast about in an effort to find "changes" to data carried over the network when changes actually aren't happening. Trust and promote strong encryption to technically protect the integrity of information flows.

-- Do not get sidetracked by advertising when thinking about what broadband providers are doing. Focus on realized speed, availability, and pricing. Endeavor to encourage greater attention to packet loss and its impact on throughput. Incent greater visibility when it comes to application throughput.

-- With respect to your questions relating to throttling and prioritization, we encourage you to review the comments previously personally filed by Dr. St Sauver in July 2014 in conjunction with the "Protecting and Promoting the Open Internet" proceeding.

Farsight Security, Inc., stands ready to address any comments or questions you may have regarding this filing.